KEY MANAGEMENT WORKSHOP AGENDA
National Institute of Standards and Technology
Building 101, Lecture Room A
November 1-2, 2001

November 1:

9:00-9:05   Welcome to the Workshop (Elaine Barker)

9:05-9:15   Overview of the History of the Key Management Project
Goals and Purpose of Workshop
Goals and Purpose of the Key Establishment Schemes Document (Elaine Barker)

Document under discussion: Key Establishment Schemes

9:15-10:15   Overview of the Key Establishment Schemes Document (Miles Smid)

10:15-10:30   Break

10:30-11:30   Issues and Discussions (Second Pass, Elaine Barker and Miles Smid) - See attachment

11:30-12:30   Lunch

12:30-1:30   Issues and Discussion (contd.) (Second Pass, Elaine Barker and Miles Smid)

1:30-2:00   Final Discussion and New Items (Elaine Barker and Miles Smid)

2:00-2:15   Break

2:15-3:15   Status of Draft ANSI X9.44 (Burt Kaliski)

3:15-3:45   Future Plans (Elaine Barker)

3:45-4:00   Break

Document under discussion: Key Management Guideline

4:00-4:15   Overview of the Goals and Purpose of the Key Management Guideline
(Elaine Barker)

4:15-4:45   Overview of the Key Management Guideline (Curt Barker)

4:45   Close for the day

November 2: Document under discussion: Key Management Guideline

9:00-9:30   Introduction, Glossary, and Acronyms (Tim Polk)

9:30-10:30   Cryptographic Algorithms, Keys, and Other Keying Material (Miles Smid)

10:30-10:45   Break

10:45-11:45   Key Management Lifecycle (Curt Barker, Miles Smid)

11:45-12:45   Lunch

12:45-1:45   Key Management Lifecycle Continued (Curt Barker)

1:45-2:45   General Key Management Guidance (Elaine. Barker)

2:45-3:00   Break

3:00-3:30   Key Management Guidance-Selected Infrastructures (Tim Polk)

3:30-4:30   Key Management Guidance-Selected Protocols and Applications (Bill Burr)

4:30-5:00   Final Discussion and New Items (Curt Barker, Elaine Barker, Bill Burr, Tim Polk, Miles Smid)

5:00-5:15   Future Plans (Elaine Barker)

5:15   Close

Attachment
Discussion Issues for the Key Establishment Schemes Document

1. Are there any situations that are not addressed by at least one of the schemes in this document?
2. Which schemes should use key confirmation?
3. Should key confirmation ever be mandatory?
4. Does it unnecessarily hinder any application to require a distinction between the initiator and responder in a key agreement scheme?
5. Should the identities of the initiator and responder be used in the calculation of shared secrets? (Related to question 4).
6. Should this document address broader forms of key derivation (e.g., key derivation for multi-user applications)?
7. What are the most important key establishment scheme attributes, and how should they be presented? (Please bring your ideas)
8. Are there any additional topics that should be covered?
9. Are there any additional appendices that should be included?